대 한 민 국 특 허 청

KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2001년 제 54398 호
Application Number PATENT-2001-0054398

출 원 년 월 일 : 2001년 09월 05일
Date of Application SEP 05, 2001

출 원 인 : 한국전자통신연구원
Applicant(s) KOREA ELECTRONICS & TELECOMMUNICATIONS RESEARCH INST

2001 년 10 월 05 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【참조번호】 0001

【제출일자】 2001.09.05

【발명의 명칭】 네트워크간의 침입에 대응하기 위한 보안 시스템 및 그 방법

【발명의 영문명칭】 Security System against intrusion among networks and the method

【출원인】

【명칭】 한국전자통신연구원

【출원인코드】 3-1998-007763-8

【대리인】

【명칭】 특허법인 신성

【대리인코드】 9-2000-100004-8

【지정된변리사】 변리사 정지원, 변리사 원석희, 변리사 박해천

【포괄위임등록번호】 2000-051975-8

【발명자】

【성명의 국문표기】 한민호

【성명의 영문표기】 HAN,Min Ho

【주민등록번호】 740615-1163013

【우편번호】 302-782

【주소】 대전광역시 서구 삼천동 국화아파트 601-802

【국적】 KR

【발명자】

【성명의 국문표기】 나중찬

【성명의 영문표기】 NA,Jung Chan

【주민등록번호】 620725-1408216

【우편번호】 305-755

【주소】 대전광역시 유성구 어은동 한빛아파트 121동 206호

【국적】 KR

【발명자】

【성명의 국문표기】	손승원
【성명의 영문표기】	SOHN,Sung Won
【주민등록번호】	571225-1674514
【우편번호】	305-762
【주소】	대전광역시 유성구 전민동 엑스포아파트 208-902
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 특허법인 신성 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	9	면	9,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	9	항	397,000 원
【합계】	435,000 원		
【감면사유】	정부출연연구기관		
【감면후 수수료】	217,500 원		
【첨부서류】	1. 요약서·명세서(도면)_1통		

【요약서】

【요약】

1. 청구범위에 기재된 발명이 속한 기술분야

본 발명은 네트워크간의 침입에 대응하기 위한 보안 시스템 및 그 방법과상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것임.

2. 발명이 해결하려고 하는 기술적 과제

본 발명은, 전체 네트워크 차원에서 서로 다른 네트워크간 침입 탐지 정보를 공유하여 침입에 대한 추적을 통해 침입자가 속해 있는 네트워크에서의 대응을 수행하는 보안 시스템 및 그 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공함.

3. 발명의 해결방법의 요지

본 발명은, 네트워크상의 보안 시스템에 있어서, 패킷을 분석하여 침입을 탐지한 후, 침입과 관련된 정보를 첨부해 엑티브 패킷을 생성하여 침입자 패킷의 송신자 주소로 전송하는 침입탐지수단; 및 침입자가 지나온 전체 네트워크 경로에 대해, 상기 침입탐지수단으로부터의 엑티브 패킷을 통해 침입을 추적하고, 침입자와 관련된 패킷을 필터링하여 고립시키는, 피 공격자 및 침입자의 로컬 네트워크상의 엑티브 노드로 구성된 라우팅 수단을 포함함.

4. 발명의 중요한 용도

본 발명은 네트워크간의 침입에 대응하기 위한 보안 시스템 등에 이용됨.

【대표도】

도 1

【색인어】

침입 탐지 시스템, 로컬 네트워크 보더 라우터, 패킷 필터링, 엑티브 패킷, IP 스프핑

【명세서】

【발명의 명칭】

네트워크간의 침입에 대응하기 위한 보안 시스템 및 그 방법{Security System against intrusion among networks and the method}

【도면의 간단한 설명】

도 1 은 본 발명에 따른 보안 시스템의 일실시예 전체 구조도.

도 2 는 본 발명에 따른 로컬 네트워크의 보더 라우터의 패킷 필터링 기능을 나타낸 일실시예 설명도.

도 3 은 본 발명에 따른 상기 도 1 의 침입 탐지 시스템의 일실시예 상세 구조도.

도 4 는 본 발명에 따른 침입 탐지 시스템의 일실시예 상세 흐름도.

도 5 는 본 발명에 따른 상기 도 1 의 로컬 네트워크의 보더 라우터의 일실시예 구조도.

도 6 은 본 발명에 따른 로컬 네트워크의 보더 라우터의 일실시예 상세 흐름도.

도 7 은 본 발명이 적용되는 인터넷 망의 구조 설명도.

도 8 은 본 발명에 따른 보안 시스템 내의 침입에 대한 대응과정을 나타낸 일실시예 설명도.

도 9 는 본 발명에 따른 보안 시스템 외부로부터의 침입에 대한 대응과정을 나타낸 다른 일실시예 설명도.

도 10 은 본 발명에 따른 다른 호스트(서버)를 경유한 침입 및 대응 과정을 나타낸 또 다른 일실시예 설명도.

* 도면의 주요 부분에 대한 부호의 설명

101 : 인터넷 102 : 로컬 네트워크 보더 라우터

103 : 침입 탐지 시스템

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<14> 본 발명은 네트워크간의 침입에 대응하기 위한 보안 시스템 및 그 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.

<15> 최근 많은 정보 보호 시스템에서는 보안의 문제를 해결하기 위해 다양한 보안 장비들이 설치되고 있고, 현재는 침입차단, 침입탐지 등 네트워크 및 서버의 보안을 책임지는 다양한 구성 요소들이 결합되어 보다 침입 징후에 대한 협조 및 연계성을 부여하는 통합 보안 솔루션이 제시되고 있다. 그러나, 이러한 보안 시스템은 모두가 로컬 네트워크 차원에서 침입을 탐지하고 이에 대한 개별적인 대

응을 가하는 반면에, 공격자에 대해 전체 네트워크 차원에서의 대응이 불가능하다. 따라서, 서로 다른 네트워크 시스템간 침입 탐지 정보를 공유하고 이를 통해 모든 시스템 환경에서 일정한 대응을 유도해 내기 위한 인프라의 구축이 시급한 현실이다.

<16> 현재의 이러한 시스템적 대응 한계를 극복하기 위한 새로운 기술들이 다양하게 모색되고 있으며, 이중 주목할 만한 것으로 IDIP(Intrusion Detection and Isolation Protocol)와 DecIDUouS(Decentralized Source Identification of Intrusion Source)가 제안되었다. 그러나, 상기 기법들은 기존의 모든 네트워크 구조 변경을 요구하고 있다. 따라서, 기존의 네트워크 구조 변경을 최소화하며 침입을 탐지하고 추적하여 고립시킬 수 있는 방안이 필수적으로 요구된다.

【발명이 이루고자 하는 기술적 과제】

<17> 본 발명은, 상기한 바와 같은 요구에 부응하기 위하여 제안된 것으로, 전체 네트워크 차원에서 서로 다른 네트워크간 침입 탐지 정보를 공유하여 침입에 대한 추적을 통해 침입자가 속해 있는 네트워크에서의 대응을 수행하는 보안 시스템 및 그 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공하는데 그 목적이 있다.

【발명의 구성 및 작용】

<18> 상기 목적을 달성하기 위한 본 발명의 장치는, 네트워크상의 보안 시스템에 있어서, 패킷을 분석하여 침입을 탐지한 후, 침입과 관련된 정보를 첨부해 엑티브 패킷을 생성하여 침입자 패킷의 송신자 주소로 전송하는 침입탐지수단; 및 침입자가 지나온 전체 네트워크 경로에 대해, 상기 침입탐지수단으로부터의 엑티브 패킷을 통해 침입을 추적하고, 침입자와 관련된 패킷을 필터링하여 고립시키는, 피 공격자 및 침입자의 로컬 네트워크상의 엑티브 노드로 구성된 라우팅 수단을 포함하는 것을 특징으로 한다.

<19> 또한, 본 발명의 방법은, 보안 시스템에 적용되는 보안 방법에 있어서, 침입 탐지 시스템에서 패킷을 분석하여 침입을 탐지한 후, 침입과 관련된 정보를 첨부해 엑티브 패킷을 생성하여 침입자 패킷의 송신자 주소로 전송하는 제 1 단계; 및 침입자가 지나온 전체 네트워크 경로 상에서, 엑티브 노드로 구성된 각 로컬 네트워크 보더 라우터간에 침입 탐지 정보를 공유하여 침입에 대한 추적을 통해 침입자가 속해 있는 네트워크에서의 대응을 수행하는 제 2 단계를 포함하는 것을 특징으로 한다.

<20> 한편, 본 발명은, 프로세서를 구비한 보안 시스템에, 침입 탐지 시스템에서 패킷을 분석하여 침입을 탐지한 후, 침입과 관련된 정보를 첨부해 엑티브 패킷을 생성하여 침입자 패킷의 송신자 주소로 전송하는 제 1 기능; 및 침입자가 지나온 전체 네트워크 경로 상에서, 엑티브 노드로 구성된 각 로컬 네트워크 보더 라우터간에 침입 탐지 정보를 공유하여 침입에 대한 추적을 통해 침입자가 속해 있는

네트워크에서의 대응을 수행하는 제 2 기능을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

<21> 상기와 같이 본 발명은 기존의 로컬 네트워크가 아닌 서로 다른 네트워크간 침입 탐지 정보를 공유하여 침입에 대해 추적을 통해 침입자가 속해있는 네트워크에서의 대응을 수행하는 보안 시스템 구조이다.

<22> 현재의 보안 시스템은 모두가 로컬 네트워크 차원에서 침입을 탐지하고 이에 대한 개별적인 대응을 가한다. 따라서 서로 다른 네트워크 시스템간 침입 탐지 정보를 공유하고 이를 통해 모든 시스템 환경에서 일정한 대응을 유도해 내기 위한 인프라의 구축이 시급한 현실이다. 이러한 시스템적 대응 한계를 극복하기 위한 새로운 기술들이 다양하게 모색되고 있으며, 이중 주목할 만한 것으로 IDIP(Intrusion Detection and Isolation Protocol)와 DecIdUouS(Decentralized Source) Identification of Intrusion Source)가 제안 되었다. 그러나 이를 수행하기 위해서는 기존의 모든 네트워크 구조 변경을 요구하고 있다. 따라서 본 발명에서는 기존의 패킷 필터링 기술과 엑티브 네트워크의 기술을 이용하여, 기존의 네트워크 구조 변경을 최소화하여 침입을 탐지하고 추적하여 고립시킬 수 있는 방안을 포함한다. 패킷 필터링 기술과 엑티브 네트워크의 기술을 상세히 설명하면 다음과 같다.

<23> 상기의 패킷 필터링 기술은 침입에 대한 대응 및 IP 스프핑(IP Spoofing)의 방지를 통한 침입자의 추적이 가능하도록 하는 기능으로서, 패킷의 목적지 주소, 패킷의 송신지 주소 또는 서비스 포트번호를 기준으로 패킷 전송을 중단 또는

전송을 결정하는 작업이며, 일반적으로 라우터는 자신을 경유하는 패킷 유형별로 전송여부를 규정한 패킷 필터링 테이블을 가지고 수신 또는 송신되는 모든 패킷의 헤더 정보를 검색하여 패킷 필터링 테이블 정보들과 비교 검색한 후, 설정된 규칙에 따라 패킷을 전송 거절 또는 전송 진행을 수행하는 기술이다.

<24> 상기의 엑티브 네트워크 기술은, 기존의 네트워크의 중간노드에서 단순히 패킷의 헤더만을 보고 저장한 후 포워딩(store and forwarding)하는 식의 단순 처리를 하는 것과는 달리, 사용자가 원하는 프로그램을 패킷 내에 가지고 있거나 혹은 중간 노드에서 일부 특별한 관리자가 미리 제공하는 프로그램을 중간 노드(엑티브 노드)에서 실행하여 단순한 처리를 넘어서는 매우 다양하고 유동적인 처리를 행할 수 있는 기술이다.

<25> 상술한 목적, 특징들 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명한다.

<26> 도 1 은 본 발명에 따른 보안 시스템의 일실시예 전체 구조도이다.

<27> 도 1 에 도시된 바와 같이, 로컬 네트워크(104)의 보안 시스템은 크게 엑티브 패킷(Active Packet)을 생성하고 인식할 수 있는 침입 탐지 시스템(Intrusion Detection System : IDS)(102)들과 엑티브 노드(Active Node)로 구성된 로컬 네트워크의 보더 라우터(Local Network Boreder Router)(103)들로 구성되어 있다.

<28> 각 로컬네트워크상의 침입 탐지 시스템(102)은 패킷을 분석하여 침입을 탐지한 후, 침입과 관련된 정보를 첨부해 엑티브 패킷을 생성하여 침입자 패킷의 송신자 주소로 전송한다.

<29> 피 공격자 및 침입자의 각 로컬 네트워크상의 보더 라우터(103)는 엑티브 노드로 구성되며, 침입자가 지나온 전체 네트워크 경로에 대해, 상기 침입탐지수단으로부터의 엑티브 패킷을 통해 침입을 추적하고, 침입자와 관련된 패킷을 필터링하여 고립시킨다.

<30> 도 2 는 본 발명에 따른 로컬 네트워크의 보더 라우터의 패킷 필터링 기능을 나타낸 일시시예 설명도이다.

<31> 도 2 에 도시된 바와 같이, 모든 침입은 로컬 네트워크에서 시작되므로 각 로컬 네트워크 보더 라우터(border router)(202)는 필터링 기능을 이용하여 자기 자신의 네트워크 주소(network address)와 다른 패킷을 외부로 전송하지 않는다면, IP 스프핑을 막을 수 있고, 또한 침입을 탐지한 시스템은 어느 로컬 네트워크에서 침입이 시작되었는지 알 수 있다.

<32> 일단 침입 탐지 시스템이 침입을 탐지 했을 경우 피 공격자가 속해있는 로컬 네트워크의 대응 시스템(보더 라우터) 및 침입자가 속해있는 네트워크의 대응 시스템(보더 라우터)에게 이 정보를 알려 준다. 각 로컬 네트워크 보더 라우터가 엑티브 노드이고 침입 탐지 시스템은 엑티브 패킷을 생성할 수 있다면, 각 로컬 네트워크 보더 라우터(침입을 당한 로컬 네트워크 보더 라우터, 침입자가 속해 있는 로컬 네트워크의 보더 라우터)는 필터링을 수행하여 침입에 대한 전체 네트워크 차원에서 대응을 할 수 있다. 왜냐하면 침입 탐지 시스템은 엑티브 패

킷에 침입자 정보(여기서 침입자 정보란 IP address, port number이고, 이하 생략하겠음.)를 넣어 침입자 패킷의 송신자 주소로 전송하는 과정에서 침입자가 지나온 경로를 지나갈 때 각 로컬 네트워크의 보더 라우터는 침입 탐지 시스템에서 생성되는 엑티브 패킷을 인식하여 대응할 수 있기 때문이다.

<33> 도 3 은 본 발명에 따른 상기 도 1 의 침입 탐지 시스템의 일실시예 상세 구조도이다.

<34> 도 3 에 도시된 바와 같이, 본 발명의 침입 탐지 시스템은 기존의 침입 탐지 시스템에 비해 엑티브 패킷 프로세싱 모듈(Active Packet Processing Module)(304)기능이 추가된다.

<35> 본 발명의 침입 탐지 시스템의 구조를 상세히 설명하면 다음과 같다.

<36> 패킷 콜렉터(Packet Collector)(303)는 데이터 링크(301)를 지나가는 패킷을 모아 룰 매칭 모듈(Rule Matching Module)(302)로 전달하는 기능을 한다.

<37> 룰 매칭 모듈(302)은 패킷 콜렉터(303)로부터 패킷을 받아 분석한 후, 침입 징후와 관련있는 패킷이면 침입 징후 정보를, 엑티브 패킷이면 엑티브 패킷을 엑티브 패킷 프로세싱 모듈(304)로 전달하는 기능을 한다.

<38> 엑티브 패킷 프로세싱 모듈(304)은 룰 매칭 모듈(302)로부터 전달 받은 데이터가 침입 정보 관련 정보이면 침입 정보 관련 엑티브 패킷을 생성하여 IP 포워딩 엔진(305)를 통해서 다른 로컬 네트워크로 전송시키고, 룰 매칭 모듈(302)로부터 전달 받은 것이 엑티브 패킷이면, 침입 정보 관련 엑티브 패킷인가를 분

석하여, 그 결과가 인증된 서버를 통해 침입이 되었으면 서버에 이동 에이전트를 전송하여 외부로부터의 침입자에 대한 정보를 가져오는 기능을 한다.

<39> 도 4 는 본 발명에 따른 침입 탐지 시스템의 일실시예 상세 흐름도이다.

<40> 도 4 를 참조하여 본 발명의 침입 탐지 시스템의 동작 과정을 살펴보면, 먼저 패킷 콜랙터에 패킷이 존재하는가를 판단한다(402). 판단결과 패킷이 존재하면, 이 패킷이 침입 징후와 관련이 있는지, 즉 패킷이 룰에 매칭되는지를 분석하여 침입 여부를 검사한다(403). 검사결과 침입으로 판정 되면, 엑티브 패킷 프로세싱 모듈에 의해 침입 정보 관련 엑티브 패킷을 생성하여 침입자 패킷의 송신자 주소로 전송한다(404). 검사 결과 패킷이 엑티브 패킷인가를 판단하여(405), 엑티브 패킷이면 침입 정보 관련 엑티브 패킷인가를 판정한다(406). 판정결과의 패킷이 침입 관련 엑티브 패킷이면, 인증된 서버를 통해 침입이 되었는지를 판단하여(407), 인증된 서버이면 서버로 이동 에이전트를 전송하여 외부로부터의 침입자에 대한 정보를 가져온다(408).

<41> 도 5 는 본 발명에 따른 상기 도 1 의 로컬 네트워크의 보더 라우터의 일실시예 구조도이다.

<42> 도 5 에 도시된 바와 같이, 본 발명에서 제안한 로컬 네트워크의 보더 라우터 구조는 기존의 로컬 네트워크의 보더 라우터와 달리 엑티브 패킷을 수행하기 위한 엑티브 패킷 실행 환경(Active Packet Execution Environment)(501)과 패킷 필터링을 수행하기 위한 패킷 필터링 모듈(Packet Filtering Module)(504)기능이 추가된다.

<43> 본 발명의 로컬 네트워크의 보더 라우터 구조를 상세히 설명하면 다음과 같다.

<44> 패킷 필터링 모듈(504)은 로컬 네트워크의 보더 라우터로부터 들어온 패킷을 전송할 것인가 거절할 것인가를 결정하여 전송할 패킷이면 패킷 클래스파이어(Packet Classifier)(502)로 전송하는 기능을 한다.

<45> 패킷 클래스파이어(502)는 패킷 필터링 모듈(504)로부터의 패킷이 엑티브 패킷인지 IP 패킷인지를 구분하여 IP 패킷이면 IP 포워딩 엔진(IP Forwarding Engine)(503)을 통해 패킷을 포워딩 한다. 만약 이 패킷이 엑티브 패킷이면 엑티브 패킷 실행 환경(501)에서 수행되도록 전달하는 기능을 한다.

<46> 엑티브 패킷 실행 환경(501)은 패킷 클래스파이어(502)로부터의 패킷이 침입 정보 관련 패킷일 경우 패킷 필터링 모듈(504)에 필터링 해야 할 패킷 관련 정보를 삽입한 뒤, IP 포워딩 엔진(503)을 통해 패킷을 포워딩 하는 기능을 한다.

<47> 도 6 은 본 발명에 따른 로컬 네트워크의 보더 라우터의 일실시예 상세 흐름도이다.

<48> 도 6을 참조하여, 로컬 네트워크의 보더 라우터의 동작을 살펴보면, 로컬 네트워크의 보더 라우터로 들어온 패킷이 필터링을 해야할 패킷, 즉 전송할 패킷인지 거절해야 할 패킷인지를 결정한다(603). 만약, 거절해야 하는 패킷이면 패킷 필터링을 수행한다(602). 한편 전송해야 할 패킷이 IP 패킷인지 엑티브 패킷인지를 판단하여(604), 엑티브 패킷이면 엑티브 패킷 실행 환경에서 엑티브 패킷

을 수행한다(606). 이 패킷이 침입 정보 관련 엑티브 패킷인지를 판단하여(607), 침입 정보 관련 엑티브 패킷일 경우, 패킷의 침입 정보를 패킷 필터링 모듈에 삽입한 후(608), IP 포워딩 엔진(IP Forwarding Engine)을 통해 패킷을 포워딩시킨다(605). 한편, 전송해야 할 패킷이 IP 패킷이면, IP 포워드 엔진을 통해 패킷을 포워딩한다(605).

<49> 다음, 도 7, 도 8, 도 9, 도 10은 아직 모든 망의 보안 시스템이 구축 되지 않았을 경우, 후술되는 도 8의 보안 시스템 내의 로컬 네트워크에서의 침입이 발생한 경우와 도 9의 보안 시스템 외부의 로컬 네트워크에서의 침입이 발생된 경우, 그리고 도 10의 다른 호스트를 경유하여 침입을 한 경우가 존재한다. 본 발명에서는 일례로 보안 시스템이 하나의 ISP(Internet Service Provider)에서만 수행된다고 가정한다. 물론 여러 개의 ISP가 보안 시스템이 될 수 있음은 자명하다.

<50> 도 7 은 본 발명이 적용되는 인터넷 망의 구조 설명도이다.

<51> 도 7 에 도시된 바와 같이, 후술되는 도 8, 도 9, 도 10, 도 11에 공통으로 적용되는 인터넷 망 구성 설명도로서, 인터넷 망 중에서 점선 부분이 제안된 본 발명의 보안 시스템이다.

<52> 도 8 은 본 발명에 따른 보안 시스템 내의 침입에 대한 대응과정을 나타낸 일실시예 설명도이다.

<53> 도 8 에 도시된 바와 같이, 로컬 네트워크 3(805)에 속해있는 침입자가 로컬 네트워크 1(804)의 서버에 침입을 시도할 경우 로컬 네트워크 1(804)의 침입

탐지 시스템(802)이 침입을 감지하여 침입자에게로 침입자의 정보를 엑티브 패킷에 넣어 전송한다. 모든 로컬 네트워크의 보더 라우터(806)는 필터링 기능이 있으므로 침입자는 IP 스프핑을 수행할 수 없으므로 침입자가 속해 있는 로컬 네트워크까지 이 패킷은 전송될 것이다. 로컬 네트워크 1(804)의 보더 라우터는 엑티브 노드이므로 엑티브 패킷을 인식하고 수행할 수 있다. 따라서, 로컬 네트워크 3(803)로부터 전송된 침입자 패킷을 일단 필터링을 통해 막은 뒤 ISP(801)를 통해 계속 전송한다. 모든 ISP(801) 라우터는 엑티브 패킷을 인식할 수 없으므로 단지 포워딩만 수행한다. 마지막으로 이 엑티브 패킷이 침입자가 속한 로컬 네트워크 3(805)의 보더 라우터(806)에 도달하면 침입자 패킷이 더 이상 외부로 나가지 않도록 필터링을 수행한다.

<54> 도 9 는 본 발명에 따른 보안 시스템 외부로부터의 침입에 대한 대응과정을 나타낸 다른 일실시예 설명도이다.

<55> 도 9 에 도시된 바와 같이, 보안 시스템 외부로부터 로컬 네트워크 1(904)의 서버에 침입을 시도할 경우 로컬 네트워크 1(904)의 침입 탐지 시스템(902)이 침입을 감지하여 침입자에게로 침입자의 정보를 엑티브 패킷에 넣어 전송한다. 로컬 네트워크 1(904)의 보더 라우터(903)는 엑티브 노드이므로 엑티브 패킷을 인식할 수 있다. 따라서, 보안 시스템 외부로부터 전송된 침입자 패킷을 일단 필터링을 통해 막은 뒤 ISP(901)를 통해 계속 전송한다. 모든 ISP(901)라우터는 엑티브 패킷을 인식할 수 없으므로 단지 포워딩만 수행하고 결국 이 패킷이 보안 시스템 밖으로 나가게 되면 더 이상의 추적을 통한 대응은 불가능하게 된다. 따

라서, 이와 같은 경우에는 단지 침입을 탐지한 로컬 네트워크에서의 대응만 가능하다.

<56> 도 10 은 본 발명에 따른 다른 호스트(서버)를 경유한 침입 및 대응 과정을 나타낸 또 다른 일실시예 설명도이다.

<57> 도 10 에 도시된 바와 같이, 굵은선으로 표시된 부분은 로컬 네트워크 4(1004)에 속해 있는 침입자가 로컬 네트워크 3(1003)에 있는 서버(1009)를 경유하여 로컬 네트워크 1(1001)의 서버를 공격한 경우이다. 점선으로 표시된 부분은 침입에 대한 대응 경로를 나타낸 것인데, 상세히 설명하면 다음과 같다.

<58> 로컬 네트워크 1(1001)에 존재하는 침입탐지 시스템(1005)이 침입을 감지하여 침입자의 로컬 네트워크 3(1003)의 서버(1009)로 침입자의 정보를 엑티브 패킷에 넣어 전송한다. 이 과정에서 로컬 네트워크 1(1001)의 보더 라우터(1006)와 로컬 네트워크 3(1003)의 보더 라우터(1007)는 로컬 네트워크 3(1003)로부터 전송되는 침입과 관련된 패킷 필터링을 수행한다. 이 때, 로컬 네트워크 3(1003)에 존재하는 침입 탐지 시스템(1008)은 로컬 네트워크 1(1001)에서 전송된 엑티브 패킷을 분석하여 자신의 서버(1009)로부터 침입이 발생된 것을 알고 서버(1009)에 이동 에이전트(Mobile Agent)를 전송하여 외부로부터 들어온 패킷 중 로컬 네트워크 1(1001)의 서버로 전송된 패킷에 대한 정보를 가져온다. 이 정보를 이용하여 로컬 네트워크 3(1003)의 침입 탐지 시스템(1008)은 로컬 네트워크 4(1004)로부터 침입이 시작된 것을 알 수 있다. 결국 로컬 네트워크 3(1003)의 침입 탐지 시스템(1008)은 로컬 네트워크 4(1004)의 침입자 주소로, 침입자에 대한 정보를 엑티브 패킷에 넣어 전송한다. 이 과정에서 로컬 네트워크 3(1003)의 보더 라

우터(1007)와 로컬 네트워크 4(1004)의 보더 라우터(1010)는 로컬 네트워크 4(1004)로부터 저장되는 침입과 관련된 패킷 필터링을 수행한다.

<59> 상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 기록매체(씨디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다.

<60> 이상에서 설명한 본 발명은 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니고, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러가지 치환, 변형 및 변경이 가능하다는 것이 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 명백할 것이다

【발명의 효과】

<61> 상기한 바와 같은 본 발명은, 기존의 ISP는 변경하지 않고 로컬 네트워크의 보더 라우터와 침입 탐지 시스템만의 변경으로 전체 네트워크 차원에서 침입을 탐지하고 추적하여 고립시킴으로써. 기존의 방안에 비해 최소한의 수정을 통해, 침입자가 속해 있는 네트워크에서의 대응을 제공하는 효과가 있다.

【특허청구범위】

【청구항 1】

네트워크상의 보안 시스템에 있어서,

패킷을 분석하여 침입을 탐지한 후, 침입과 관련된 정보를 첨부해 엑티브 패킷을 생성하여 침입자 패킷의 송신자 주소로 전송하는 침입탐지수단; 및

침입자가 지나온 전체 네트워크 경로에 대해, 상기 침입탐지수단으로부터의 엑티브 패킷을 통해 침입을 추적하고, 침입자와 관련된 패킷을 필터링하여 고립시키는, 피 공격자 및 침입자의 로컬 네트워크상의 엑티브 노드로 구성된 라우팅 수단

을 포함하는 네트워크간의 침입에 대응하기 위한 보안 시스템.

【청구항 2】

제 1 항에 있어서,

상기 침입탐지수단은,

침입이 시작된 로컬 네트워크를 알 수 있고, 침입 탐지시 피 공격자가 속해있는 로컬 네트워크의 필터링수단 및 침입자가 속해있는 로컬 네트워크의 필터링 수단으로 침입 사실을 알려 주는 것을 특징으로 하는 네트워크간의 침입에 대응하기 위한 보안 시스템.

【청구항 3】

제 2 항에 있어서,

상기 침입탐지수단은,

지나가는 패킷을 모으기 위한 패킷 수집 수단;

상기 패킷 수집 수단으로부터 패킷을 받아 침입 징후와 관련 있는 패킷인지, 엑티브 패킷인지를 분석하기 위한 패킷 분석 수단; 및

상기의 패킷 매칭 수단으로부터 침입 정보나, 엑티브 패킷을 받아 처리하기 위한 엑티브 패킷 처리수단

을 포함하는 네트워크간의 침입에 대응하기 위한 보안 시스템.

【청구항 4】

제 3 항에 있어서,

상기 엑티브 패킷 처리수단은,

상기 패킷 분석 수단으로부터 전달받은 데이터가 침입 정보 관련 정보이면 침입 정보 관련 엑티브 패킷을 생성하여 다른 로컬 네트워크로 전송시키고, 상기 패킷 분석 수단으로부터 전달받은 것이 엑티브 패킷이면 침입 정보 관련 엑티브 패킷인가를 분석하여 그 결과가 인증된 서버를 통해 침입이 되었으면 서버에 이동 에이전트를 전송하여 외부로부터의 침입자에 대한 정보를 가져오는 것을 특징으로 하는 네트워크간의 침입에 대응하기 위한 보안 시스템.

【청구항 5】

제 1 항 내지 제 4 항 중 어느 한 항에 있어서,

상기 라우팅수단은 각각,

인입되는 패킷을 전송할 것인가 거절할 것인가를 결정하는 패킷 필터링 수단;

상기 패킷 필터링 수단으로부터 필터링된 패킷이 엑티브 패킷인지 인터넷 프로토콜(IP) 패킷인지를 구분하여, IP 패킷이면 IP 포워딩 엔진을 통해 패킷을 포워딩하고, 엑티브 패킷이면 엑티브 패킷 실행 환경에서 수행되도록 전달하는 패킷 분류 수단; 및

상기의 패킷 분류수단으로부터 분류된 패킷이 침입 정보 관련 패킷일 경우, 필터링 해야 할 패킷 관련 정보를 상기 패킷 필터링 수단에 삽입한 뒤, IP 포워딩 엔진을 통해 패킷을 포워딩시키기 위한 엑티브 패킷 실행환경 제공수단

을 포함하는 네트워크간의 침입에 대응하기 위한 보안 시스템.

【청구항 6】

보안 시스템에 적용되는 보안 방법에 있어서,

침입 탐지 시스템에서 패킷을 분석하여 침입을 탐지한 후, 침입과 관련된 정보를 첨부해 엑티브 패킷을 생성하여 침입자 패킷의 송신자 주소로 전송하는 제 1 단계; 및

침입자가 지나온 전체 네트워크 경로 상에서, 엑티브 노드로 구성된 각 로컬 네트워크 보더 라우터간에 침입 탐지 정보를 공유하여 침입에 대한 추적을 통해 침입자가 속해 있는 네트워크에서의 대응을 수행하는 제 2 단계

를 포함하는 네트워크간의 침입에 대응하기 위한 보안 방법.

【청구항 7】

제 6 항에 있어서,

상기 제 1 단계는,

패킷이 존재하는지를 판단하는 제 3 단계;

상기의 제 3 단계의 판단 결과에 따라, 존재하는 패킷이 침입 징후와 관련 있으면, 침입 정보 관련 엑티브 패킷을 생성하여 다른 로컬 네트워크로 전송시키는 제 4 단계;

상기의 제 3 단계의 판단 결과에 따라, 존재하는 패킷이 엑티브 패킷이면, 침입 정보 관련 엑티브 패킷인가를 분석하는 제 5 단계; 및

상기 제 5 단계의 분석 결과 인증된 서버를 통해 침입되었으면, 서버에 이동 에이전트를 전송하여 외부로부터의 침입자에 대한 정보를 가져오는 제 6 단계

를 포함하는 네트워크간의 침입에 대응하기 위한 보안 방법.

【청구항 8】

제 6 항 또는 제 7 항에 있어서,

상기 제 2 단계는,

로컬 네트워크 보더 라우터로 들어온 패킷이 필터링에 의해 전송할 패킷이면, 엑티브 패킷인지, IP 패킷이지를 판단하는 제 7 단계;

상기 제 7 단계의 판단 결과, IP 패킷이면 패킷을 포워딩 시키는 제 8 단계; 및

상기 제 7 단계의 판단 결과, 엑티브 패킷이면 침입 정보 관련 패킷인지를 판단하여, 침입 정보 관련 패킷일 경우 침입 정보 관련 정보를 저장 후 패킷을 포워딩시키는 제 9 단계

를 포함하는 네트워크간의 침입에 대응하기 위한 보안 방법.

【청구항 9】

프로세서를 구비한 보안 시스템에,

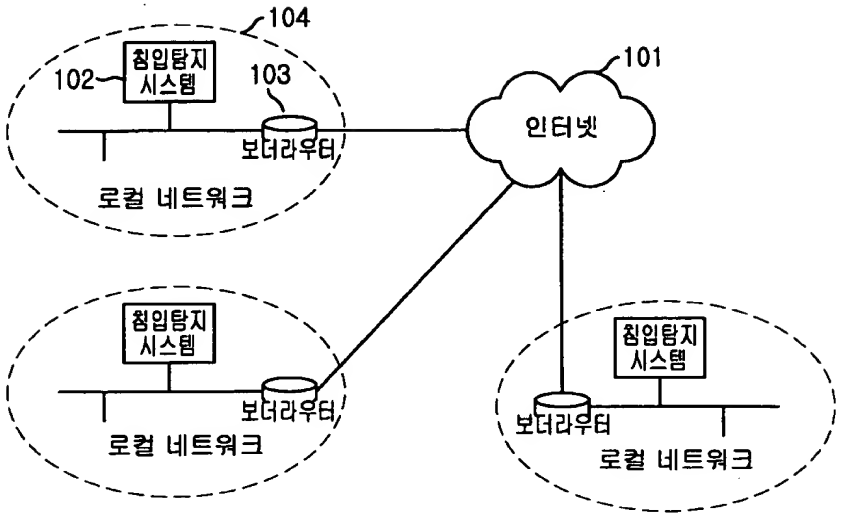
침입 탐지 시스템에서 패킷을 분석하여 침입을 탐지한 후, 침입과 관련된 정보를 첨부해 엑티브 패킷을 생성하여 침입자 패킷의 송신자 주소로 전송하는 제 1 기능; 및

침입자가 지나온 전체 네트워크 경로 상에서, 엑티브 노드로 구성된 각 로컬 네트워크 보더 라우터간에 침입 탐지 정보를 공유하여 침입에 대한 추적을 통해 침입자가 속해 있는 네트워크에서의 대응을 수행하는 제 2 기능

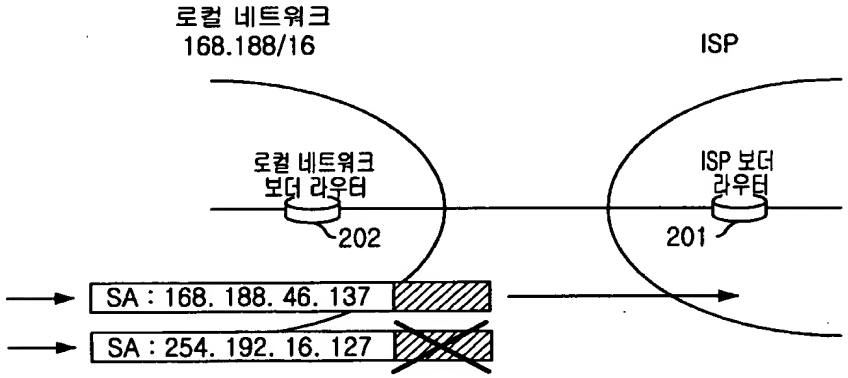
을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【도면】

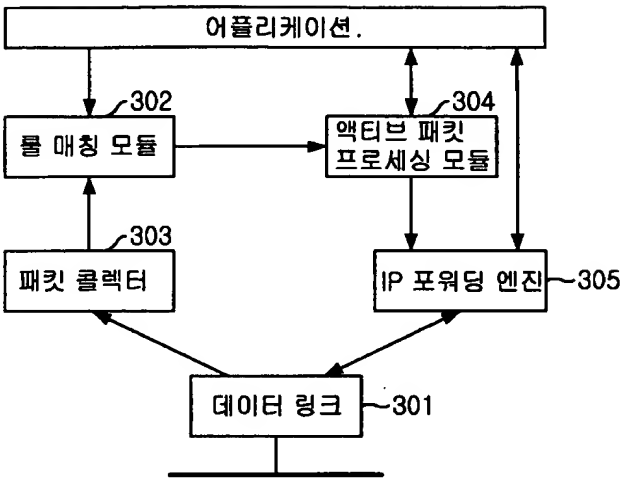
【도 1】


104
침입탐지 시스템
102
103
보더라우터
로컬 네트워크
101
인터넷
침입탐지 시스템
보더라우터
로컬 네트워크
침입탐지 시스템
보더라우터
로컬 네트워크

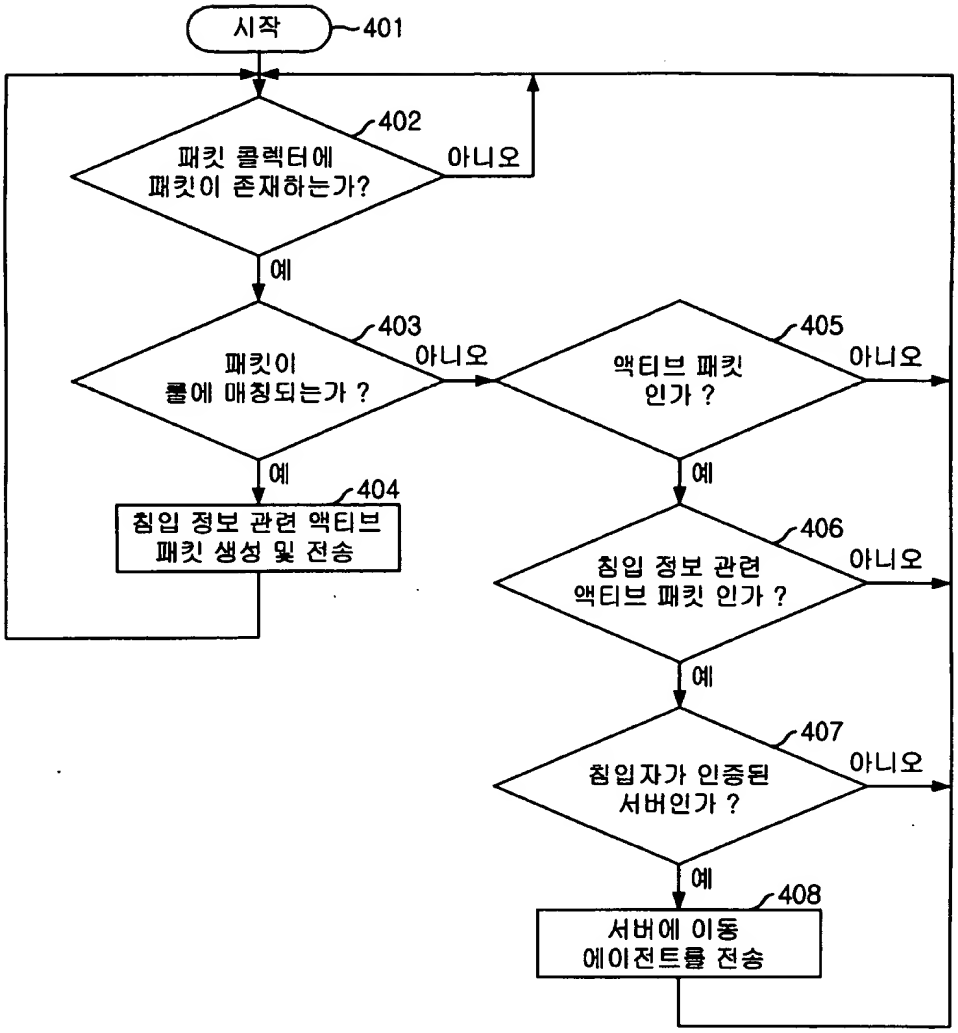
【도 2】


로컬 네트워크
168.188/16
ISP
로컬 네트워크
보더 라우터
202
ISP 보더
라우터
201
SA : 168. 188. 46. 137
SA : 254. 192. 16. 127

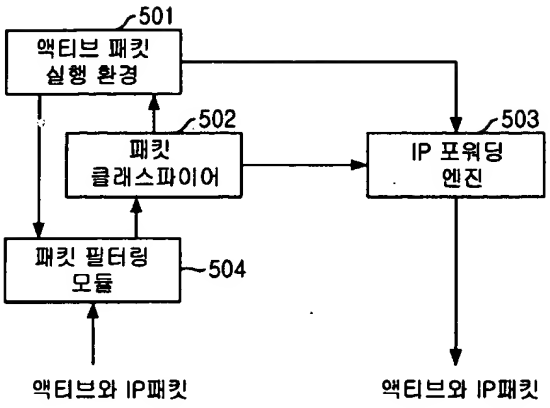
【도 3】


어플리케이션.
302
룰 매칭 모듈
304
액티브 패킷 프로세싱 모듈
303
패킷 콜렉터
IP 포워딩 엔진
305
데이터 링크
301

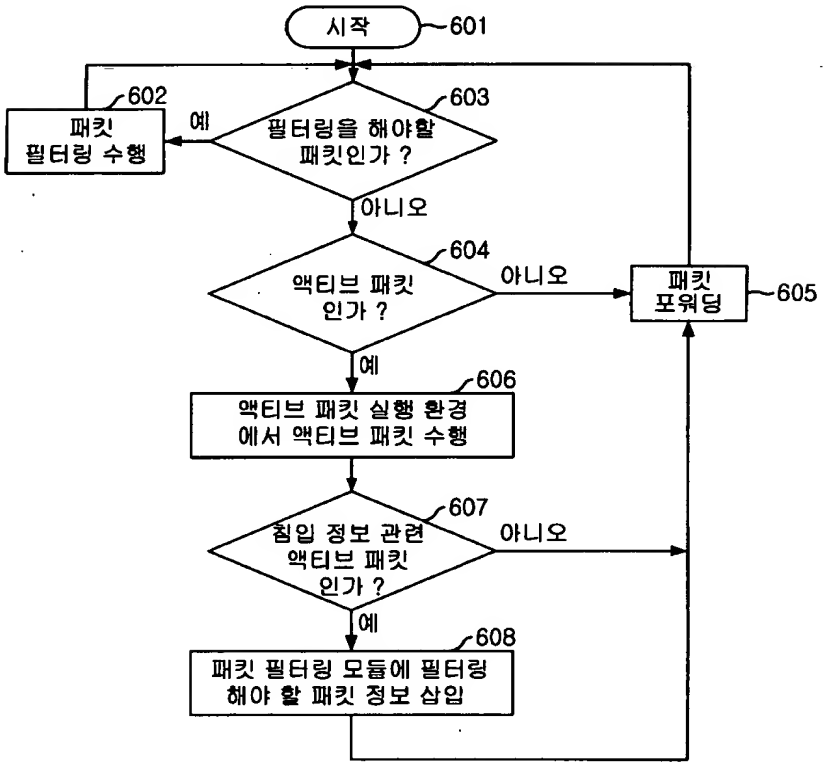
【도 4】


시작
401
402
패킷 콜렉터에 패킷이 존재하는가?
아니오
예
403
패킷이 룰에 매칭되는가 ?
아니오
405
액티브 패킷 인가 ?
아니오
예
404
침입 정보 관련 액티브 패킷 생성 및 전송
406
침입 정보 관련 액티브 패킷 인가 ?
아니오
예
407
침입자가 인증된 서버인가 ?
아니오
예
408
서버에 이동 에이전트를 전송

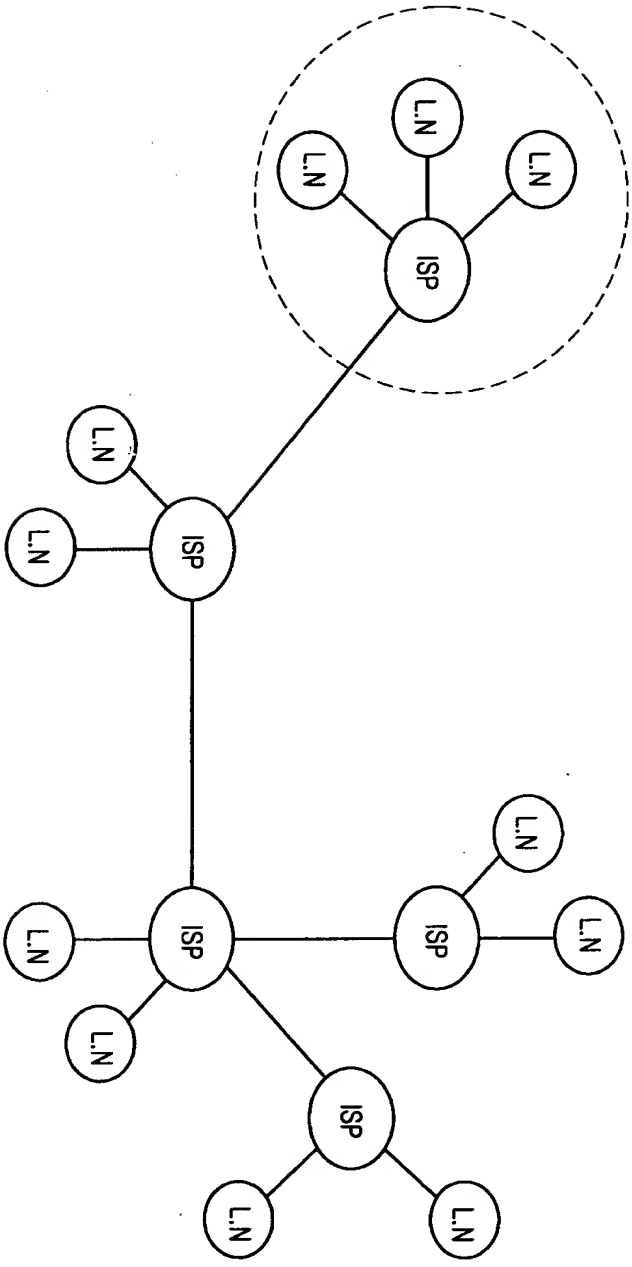
【도 5】


501
액티브 패킷 실행 환경
502
패킷 클래스파이어
503
IP 포워딩 엔진
패킷 필터링 모듈
504
액티브와 IP패킷
액티브와 IP패킷

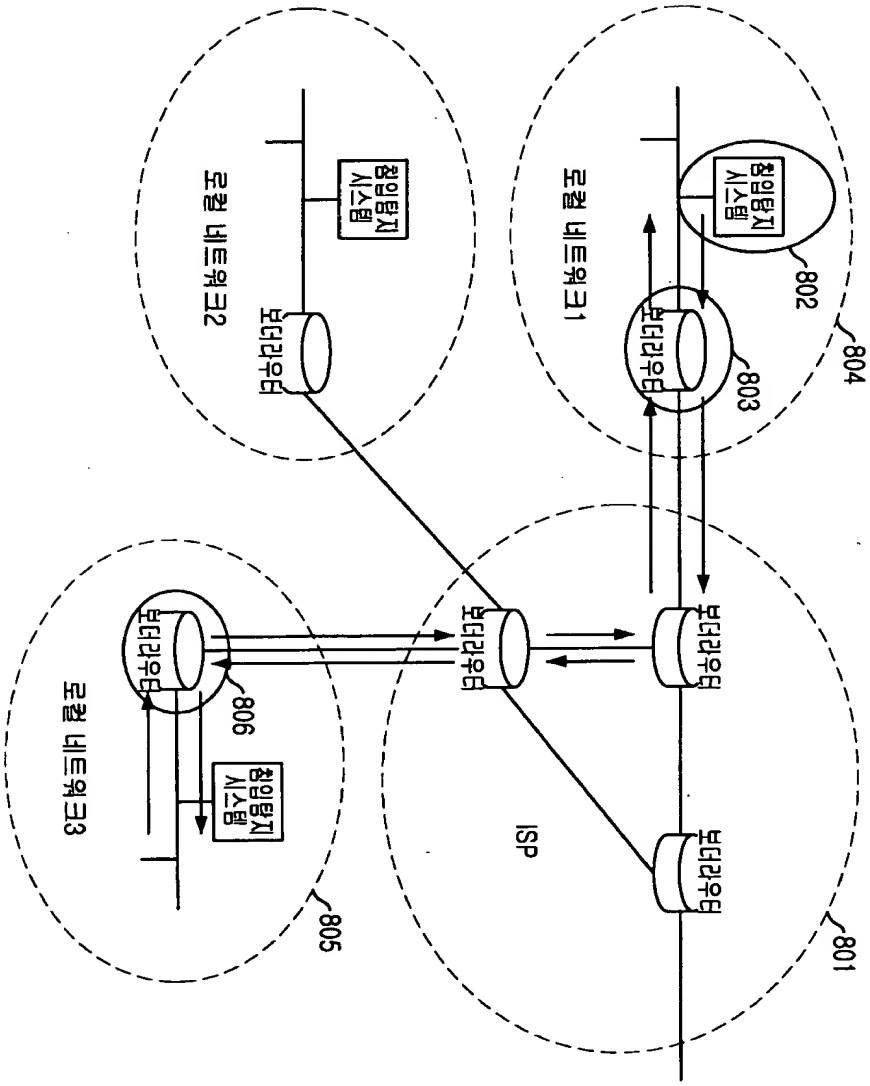
【도 6】


시작
601
602
패킷 필터링 수행
예
603
필터링을 해야할 패킷인가 ?
아니오
604
액티브 패킷 인가 ?
아니오
패킷 포워딩
605
예
606
액티브 패킷 실행 환경에서 액티브 패킷 수행
607
침입 정보 관련 액티브 패킷 인가 ?
아니오
예
608
패킷 필터링 모듈에 필터링 해야 할 패킷 정보 삽입

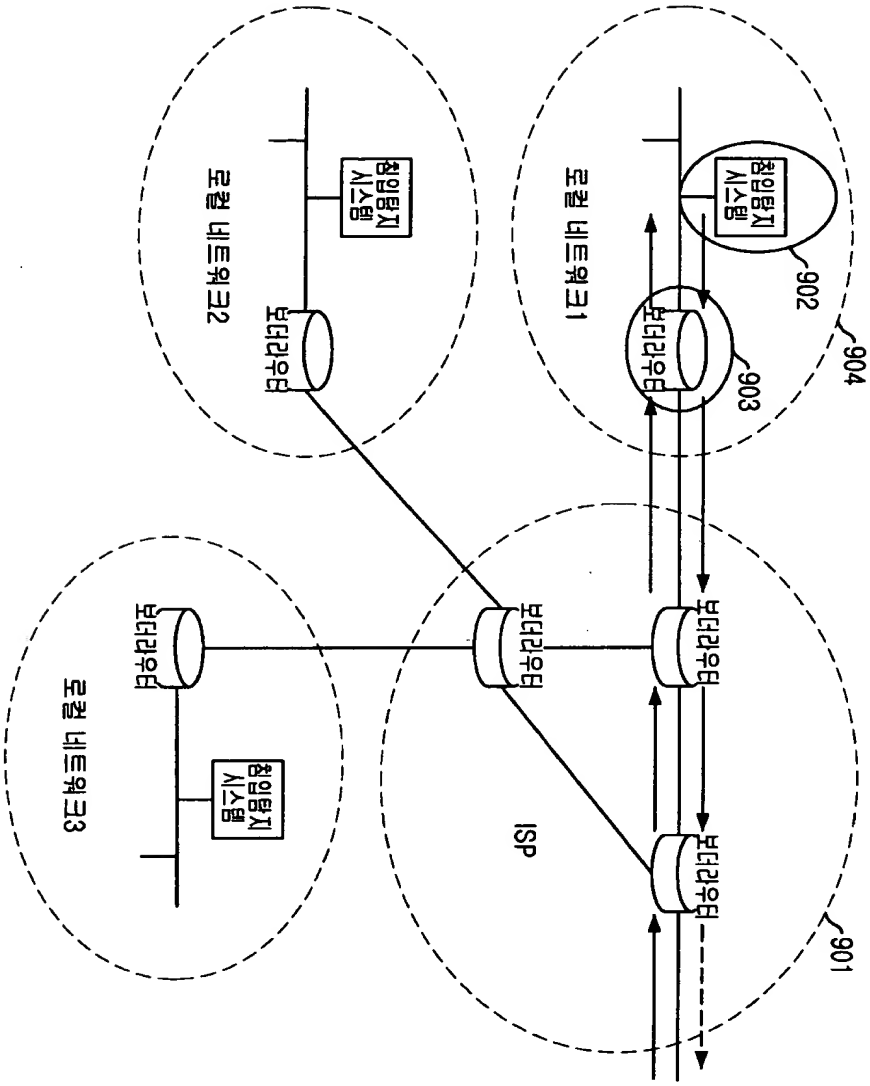
【도 7】



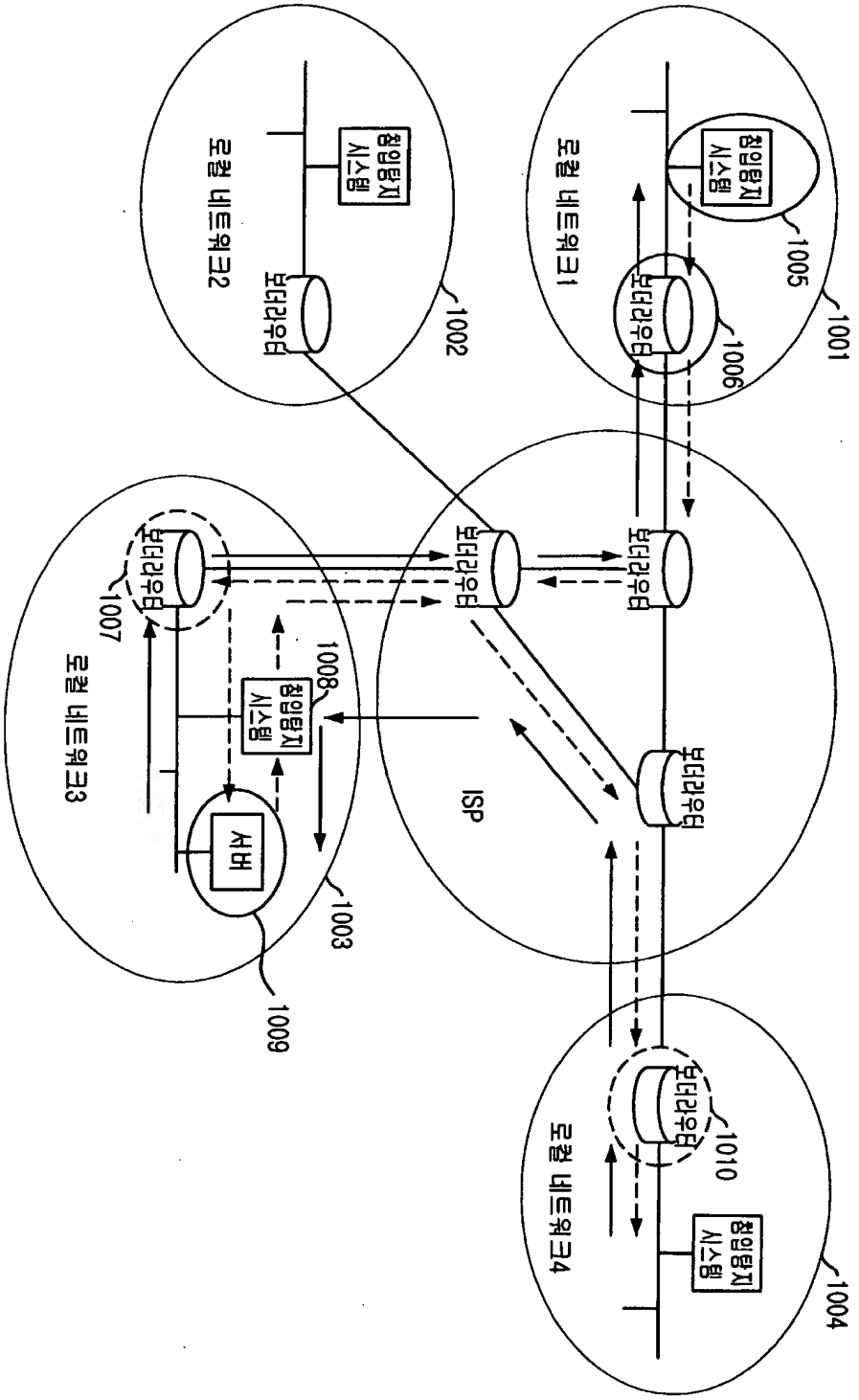
【도 8】


로컬 네트워크2
웹페이지 시스템
로컬 네트워크1
웹페이지 시스템
802
804
803
로컬 네트워크3
806
웹페이지 시스템
805
ISP
801

【도 9】


로컬 네트워크2
체임탑지 시스템
로컬 네트워크1
체임탑지 시스템
902
904
903
로컬 네트워크3
체임탑지 시스템
ISP
901

【도 10】


로컬 네트워크1
로컬 네트워크2
로컬 네트워크3
로컬 네트워크4
ISP
라우터
체인탐지 시스템
서버
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010